

20230427-A001

What is claimed is:

- 1 1. A system for providing public key cryptography including
2 assistance in recovery of messages sent to users, the method comprising:
3 a first key pair generated for a particular user, the first key pair comprising
4 a public key employed for encrypting messages sent to the particular user and
5 comprising a private key employed for decrypting messages which have been
6 encrypted using the public key of the first key pair;
7 a second key pair generated for message recovery, the second key pair
8 comprising a public key employed for recovering messages which have been
9 encrypted using the public key of the first key pair and comprising a private key
10 employed for decrypting messages which have been encrypted using the public
11 key of the second key pair;
12 information referencing the public key of the second key pair embedded
13 within the public key of the first key pair; and
14 an encryption module automatically employing the public key of the
15 second key pair during encryption of the message under the public key of the first
16 key pair so that the message being encrypted can be directly decrypted using the
17 private key of the second key pair.

- 1 2. A system according to Claim 1, further comprising:
2 information which uniquely identifies the public key of the second key
3 pair stored into the public key of the first key pair.

- 1 3. A system according to Claim 2, wherein said information which
2 uniquely identifies the public key of the second key pair includes information
3 pointing to a location where the second key pair is stored.

- 1 4. A system according to Claim 1, further comprising:
2 a copy of the public key of the second key pair embedded within the
3 public key of the first key pair.

- 1 5. A system according to Claim 1, further comprising:

2 assertion information appended to the public key of the first key pair, said
3 assertion information including a pointer which uniquely identifies the public key
4 of the second key pair.

1 6. A system according to Claim 5, wherein said assertion information
2 includes constraints specifying use of the public key of the first key pair.

1 7. A system according to Claim 6, wherein the constraints include a
2 constraint specifying that use of the public key of the second key pair is
3 mandatory during encryption of a message using the public key of the first key
4 pair.

1 8. A system according to Claim 1, wherein at least one key pair
2 comprises a Diffie-Hellman-compatible key pair.

1 9. A system according to Claim 1, wherein at least one key pair
2 comprises an RSA-compatible key pair.

1 10. A system according to Claim 1, wherein said message being
2 encrypted comprises a selected one of a text file and a binary file.

1 11. In a computer system providing public key cryptography, a method
2 for assisting with recovery of messages sent to users, the method comprising:
3 generating a first key pair for a particular user, the first key pair
4 comprising a public key employed for encrypting messages sent to the particular
5 user and comprising a private key employed for decrypting messages which have
6 been encrypted using the public key of the first key pair;

7 generating a second key pair for message recovery, the second key pair
8 comprising a public key employed for recovering messages which have been
9 encrypted using the public key of the first key pair and comprising a private key
10 employed for decrypting messages which have been encrypted using the public
11 key of the second key pair;

12 embedding within the public key of the first key pair information
13 referencing the public key of the second key pair; and

14 automatically employing the public key of the second key pair during
15 encryption of the message under the public key of the first key pair so that the
16 message being encrypted can be directly decrypted using the private key of the
17 second key pair.

1 12. A method according to Claim 11, further comprising:
2 storing information which uniquely identifies the public key of the second
3 key pair.

1 13. A method according to Claim 12, wherein said information which
2 uniquely identifies the public key of the second key pair includes information
3 pointing to a location where the second key pair is stored.

1 14. A method according to Claim 11, further comprising:
2 storing a copy of the public key of the second key pair embedded within
3 the public key of the first key pair.

1 15. A method according to Claim 11, further comprising:
2 appending assertion information to the public key of the first key pair, said
3 assertion information including a pointer which uniquely identifies the public key
4 of the second key pair.

1 16. A method according to Claim 15, wherein said assertion
2 information includes constraints specifying use of the public key of the first key
3 pair.

1 17. A method according to Claim 16, wherein the constraints include a
2 constraint specifying that use of the public key of the second key pair is
3 mandatory during encryption of a message using the public key of the first key
4 pair.

1 18. A method according to Claim 11, wherein at least one key pair
2 comprises a Diffie-Hellman-compatible key pair.

1 19. A method according to Claim 11, wherein at least one key pair
2 comprises an RSA-compatible key pair.

1 20. A method according to Claim 11, wherein said message being
2 encrypted comprises a selected one of a text file and a binary file.

1 21. A computer-readable storage medium holding code for performing
2 the method according to Claims 11, 12, 14 and 15.

1 22. A public key encryption system integrating a message recovery
2 key, comprising:

3 a session encryption module block-cipher encrypting a plaintext message
4 into ciphertext using a session key;

5 a public key encryption module encrypting the session key using a public
6 key of a user, the public key of the user being associated with a private key
7 generated simultaneously thereto and encrypting the session key using a public
8 key of a message recovery agent automatically triggered upon use of the public
9 key of the user, the public key of the message recovery agent being associated
10 with a private key generated simultaneously thereto; and

11 a digital envelope forming an encrypted message comprising the
12 ciphertext and the encrypted session key.

1 23. A system according to Claim 22, further comprising:

2 a public key decryption module decrypting the encrypted message by the
3 user, by decrypting the encrypted session key using the private key of the user and
4 block-cipher decrypting the ciphertext using the decrypted session key.

1 24. A system according to Claim 22, further comprising:

2 a public key decryption module decrypting the encrypted message by the
3 message recovery agent, by decrypting the encrypted session key using the private
4 key of the message recovery agent and block-cipher decrypting the ciphertext
5 using the decrypted session key.

1 25. A system according to Claim 22, further comprising:
2 a reference stored into the public key of the user to automatically use the
3 public key of the message recovery agent upon use of the public key of the user.

1 26. A system according to Claim 25, further comprising:
2 the public key of the message recovery agent embedded as the reference
3 into the public key of the user.

1 27. A system according to Claim 25, further comprising:
2 a pointer to the public key of the message recovery agent embedded as the
3 reference into the public key of the user.

1 28. A system according to Claim 27, further comprising:
2 at least one of a cryptographic hash and a message digest of the pointer
3 stored as the reference to the public key of the message recovery agent.

1 29. A system according to Claim 25, further comprising:
2 a digital signature formed from the private key of the user; and
3 the reference stored into the public key of the user upon successfully
4 authenticating the digital signature.

1 30. A method for integrating a message recovery key into a public key
2 encryption system, comprising:
3 block-cipher encrypting a plaintext message into ciphertext using a
4 session key;
5 encrypting the session key using a public key of a user, the public key of
6 the user being associated with a private key generated simultaneously thereto;
7 encrypting the session key using a public key of a message recovery agent
8 automatically triggered upon use of the public key of the user, the public key of
9 the message recovery agent being associated with a private key generated
10 simultaneously thereto; and
11 forming an encrypted message comprising the ciphertext and the
12 encrypted session key.

1 31. A method according to Claim 30, further comprising:
2 decrypting the encrypted message by the user, comprising:
3 decrypting the encrypted session key using the private key of the
4 user; and
5 block-cipher decrypting the ciphertext using the decrypted session
6 key.

1 32. A method according to Claim 30, further comprising:
2 decrypting the encrypted message by the message recovery agent,
3 comprising:
4 decrypting the encrypted session key using the private key of the
5 message recovery agent; and
6 block-cipher decrypting the ciphertext using the decrypted session
7 key.

1 33. A method according to Claim 30, further comprising:
2 providing a reference into the public key of the user to automatically use
3 the public key of the message recovery agent upon use of the public key of the
4 user.

1 34. A method according to Claim 33, further comprising:
2 embedding the public key of the message recovery agent as the reference
3 into the public key of the user.

1 35. A method according to Claim 33, further comprising:
2 embedding a pointer to the public key of the message recovery agent as
3 the reference into the public key of the user.

1 36. A method according to Claim 35, further comprising:
2 storing the reference as at least one of a cryptographic hash and a message
3 digest of the pointer to the public key of the message recovery agent.

1 37. A method according to Claim 33, further comprising:

2 forming a digital signature from the private key of the user; and
3 storing the reference into the public key of the user upon successfully
4 authenticating the digital signature.

1 38. A computer-readable storage medium holding code for performing
2 the method according to Claims 30, 31, 32 and 33.

1 39. A public key encryption system with transparent message
2 recovery, comprising:
3 an encryption module block-cipher encrypting a plaintext message into
4 ciphertext using a session key and encrypting the session key using the public
5 key of a user responsive to a user request and encrypting the session key using a
6 public key of a message recovery agent automatically triggered upon the
7 encryption of the session key using the public key of the user, the public key of
8 the message recovery agent being associated with a private key generated
9 simultaneously thereto;
10 a decryption module decrypting the encrypted session key using the
11 private key of the message recovery agent; and block-cipher decrypting the
12 ciphertext into plaintext using the decrypted session key.

1 40. A system according to Claim 39, further comprising:
2 a digital signature generated from the private key of the user; and
3 a recovery module storing the association to the public key of the message
4 recovery agent into the public key of the user.

5 41. A method for transparently recovering a message in a public key
6 encryption system, comprising:
7 block-cipher encrypting a plaintext message into ciphertext using a
8 session key and encrypting the session key using the public key of a user
9 responsive to a user request;
10 encrypting the session key using a public key of a message recovery agent
11 automatically triggered upon the encryption of the session key using the public

12 key of the user, the public key of the message recovery agent being associated
13 with a private key generated simultaneously thereto;
14 decrypting the encrypted session key using the private key of the message
15 recovery agent; and
16 block-cipher decrypting the ciphertext into plaintext using the decrypted
17 session key.

1 42. A method according to Claim 41, further comprising:
2 authenticating a digital signature generated from the private key of the
3 user; and
4 storing the association to the public key of the message recovery agent
5 into the public key of the user.

1 43. A computer-readable storage medium holding code for performing
2 the method according to Claims 41 and 42.

00000000000000000000000000000000